(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
23 May 2002 (23.05.2002)

PCT

(10) International Publication Number
WO 02/41565 A1

(51) International Patent Classification[7]: H04L 9/00

(21) International Application Number: PCT/US01/43635

(22) International Filing Date:
16 November 2001 (16.11.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/249,434 16 November 2000 (16.11.2000) US

(71) Applicant and
(72) Inventor: **BROWN, Richard, Dean** [US/US]; 8814 Jim Davis Place, Austin, TX 78736 (US).

(74) Agent: **WIESE, William, D.**; Jenkens & Gilchrist, a Professional Corporation, 1445 Ross Avenue, Suite 3200, Dallas, TX 75202 (US).

(81) Designated States *(national)*: CN, JP, KP, SG, US.

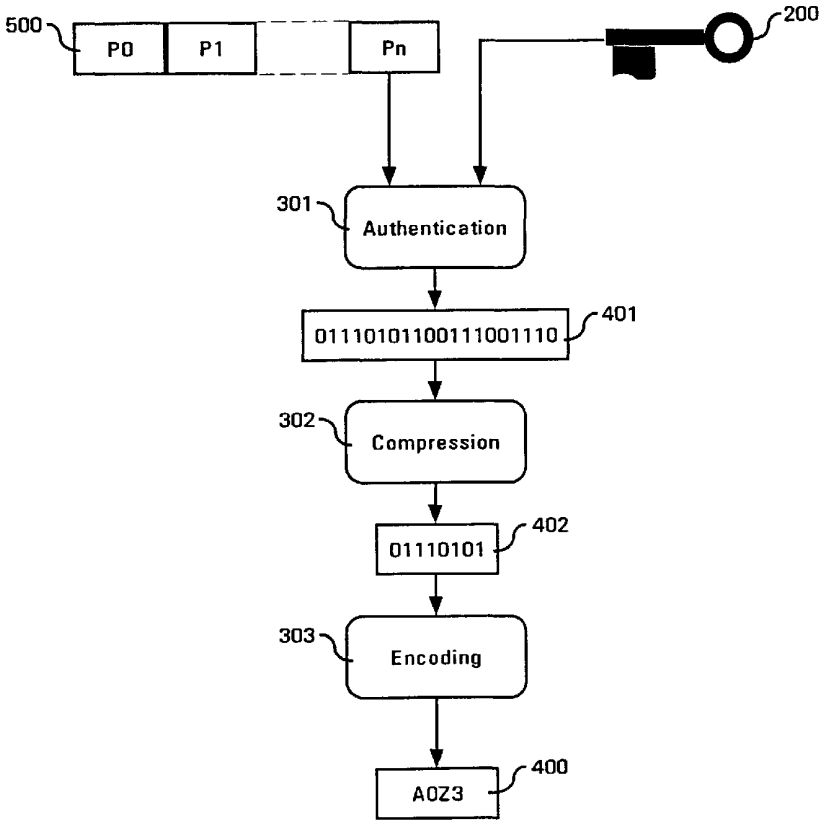
(84) Designated States *(regional)*: European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

Declaration under Rule 4.17:
— *of inventorship (Rule 4.17(iv)) for US only*

Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

[Continued on next page]

(54) Title: METHOD, SYSTEM AND DEVICES FOR AUTHENTICATING TRANSACTIONS USING VERIFICATION CODES



(57) Abstract: The present invention contemplates a system, method and devices for securing transactions by means of a transaction-dependent verification code (TVC)(400), and, in particular, an enhanced security alternative for securing card payments, having minimal impact on existing systems and networks. According to the present invention, a TVC (400) results from the compression (302) and encoding (303) of a cryptographic authentification code (401) computed from a shared secret (200) and transaction-dependent parameters (500) by means of a device (301), such as a computer system, a smart card, a mobile phone, a personal digital assistant, or a combination thereof.

WO 02/41565 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD, SYSTEM AND DEVICES FOR AUTHENTICATING TRANSACTIONS USING VERIFICATION CODES

This non-provisional application claims priority based upon prior U.S. Provisional Patent Application Serial No. 60/249,434 filed November 16, 2000 in the name of Richard Dean Brown, entitled "Securing Card Payments with a Transaction Verification Code"

FIELD

The present invention relates, generally, to the field of electronic transaction security and, more specifically, to a method, system and devices to verify the origin and the integrity of a transaction.

BACKGROUND

Fueled by the promises of the Internet, technology and service providers are urged to revamp their transaction systems to accommodate and leverage open network technologies. Unfortunately, the ubiquitous and inexpensive connectivity associated with open networks technologies comes at a higher price than initially expected. For example, securing transaction systems to accommodate an open network such as the Internet rapidly becomes a daunting task.

Among such transaction systems, online card payments have captured the attention of the electronic commerce industry. Praised as the cornerstone to the development of electronic commerce, payment transaction systems have been among the first to experience the difficulties raised by the transition to open network technologies. After more than 5 years, the transition is still incomplete. Online card fraud is reaching levels never observed before.

Card payment systems were originally designed for making face-to-face payments at the point of sale. Physical inspection of the card and matching the cardholder's signature on the sale ticket with a prototypical signature affixed to the back of the card were deemed sufficient to ascertain the authenticity and legitimacy of a payment. However, with the advent of remote transactions, such as those occurring over the telephone or the Internet, and the emergence of mobile payment devices, such as those embedded in mobile phones and other personal digital assistants, the merchants are not presented with the card and, therefore, cannot verify the authenticity of the payment instrument or the signature of the consumer.

Remote payment transactions, or "card-not-present" transactions, made their appearance more than a decade ago with the development of the mail order telephone order (MOTO) industry. To make a payment, the cardholder communicated their account number and expiration date to an operator, who keyed these pieces of information into an authorization system. This simple form of payments was rapidly subject to widespread fraud as a result of unscrupulous people charging unauthorized purchases using account numbers and expiration dates collected from sale tickets.

To mitigate MOTO fraud, the card industry developed the card verification code (CVC) which consists of a 3 or 4 digit number imprinted on the card. Because the CVC was not embossed on the card, it was intended that the CVC would not be printed by the merchant's system, thereby limiting its disclosure. Knowledge of the CVC at the time of a transaction would equate to physical possession of the card. An example of such a system can be found in U.S. Patent 6,182,894 issued Feb 6, 2001 to *Hackett, et al.*

However, CVCs are insufficient for securing transactions conducted over an open network such as the Internet. Hackers have many times demonstrated their ability to eavesdrop on open networks and break into merchant systems, thereby gaining access to the card numbers and their associated CVCs. Once known, a CVC is as easy to recite as an account number or an expiration date. Personal Identification Numbers (PINs), such as those used for securing ATM transactions and found in U.S. Patent 4,214,230 issued July 22, 1980 to *Fak, et al.*, are prone to the same attacks.

In a joint effort to address online card fraud, Visa and MasterCard proposed a new payment protocol known as Secure Electronic Transaction (SET). This protocol relies upon public key cryptography and digital certificates to authenticate cardholders with merchants and acquirers, those third-parties that maintain the merchants' credit card processing relationship, and operates as an authentication front end to existing card authorization networks and systems. Unfortunately, because it is expensive to implement and deploy, and slow to process, SET has not been, and is unlikely to be, widely adopted. SET specifications are available online from Secure Electronic Transactions LLC (www.setco.org).

Another attempt of the industry came from the ANSI X9 working group with the X9.59 standard draft proposal. Unlike SET, the X9.59 protocol specification adopts an end-to-end authentication framework where transactions are verified by card issuers, those financial institutions that issue cards to cardholders. It was intended that end-to-end authentication would remove the need for digital certificates, thereby alleviating the risk of

a compromised certificate authority and saving several hundred bytes of information in every authorization message. Unfortunately, X9.59 has other drawbacks that render its adoption unlikely. First, card issuers must adapt their account databases (schema and capacity) to store the public key of the cardholders. Second, X9.59 mandates the use of data elements not available in current protocols, thereby requiring changes in existing authorization systems and networks. Finally, X9.59 implies the use of a public key digital signature crypto-system, a process incompatible with existing card verification code infrastructures that further requires the addition of a large piece of information to each authorization message. The X9.59 draft proposal is available from the American National Standard Institute (document number DSTU X9.59-2000).

Another invention, found in U.S. Patent 5,317,636 issued May 31, 1994 to *Vizcaino*, contemplates methods and apparatus to secure card transactions by means of a secure transaction identifier, whose value cannot be determined in advance of a payment. Although this invention helps ascertain the origin of a transaction, it does no seal the transaction details necessary to a card issuer to verify the integrity of a transaction presented for authorization. An unscrupulous cardholder can later repudiate the amount to be paid; a fraudulent merchant may claim a larger amount than agreed upon with the customer; or an eavesdropper may intercept the transaction identifier and rush to obtain an authorization in advance of the legitimate merchant.

Another example of a payment security system can be found in U.S. Patent 4,630,201 issued December 16, 1986 to *White*. This invention discloses a security system for use in an electronic funds transfer environment. Checks and drafts are authenticated by a verification code that results from the combination of a transaction parameter with a pseudo random number, which is retrieved from a table stored in the payment device and determined from the sequence number of the transaction. Unfortunately, this invention only applies to systems that explicitly identify transactions in sequence, such as a check clearing system. Furthermore, this invention requires the bank to maintain a large number of random numbers per account, and only prevents tampering with the transaction amount.

The need remains for a system, method and device for use in ascertaining the origin and the integrity of a transaction. This system should have minimal requirements in term of bandwidth, storage, and computational capacity, and should be able to accommodate the infrastructures and protocols in place in legacy transaction systems.

SUMMARY

The present invention includes a system, method and devices to improve security in electronic transaction systems using a transaction-dependent verification code (TVC), which results from the compression and encoding of a cryptographic authentication code computed from transaction-dependent parameters and a secret that is shared with a verification system. The TVC is computed at a point of service by a transaction device operated by or on behalf of a user requesting access to a service delivered by an electronic transaction system. Access is only granted to the service upon the successful verification of the TVC by the verification system.

The present invention is particularly well suited for improving security in transaction systems that currently make use of static verification codes, such as PINs, passwords, and other constant pieces of information. In particular, the present invention can be used for improving security in card payment systems by replacing traditional card verification codes (CVCs) and personal identification numbers (PINs) by a TVC that complies in length and syntax with these static verification codes.

BRIEF DESCRIPTION OF THE DRAWINGS

A better understanding of the present invention may be had by reference to the drawing figures, wherein:

FIGURE 1 is a schematic view of a system according to the present invention;

FIGURE 2 is a block diagram that illustrates the method used for computation of a TVC according to the present invention;

FIGURE 3 is a block diagram that illustrates the operations of a transaction device according to the present invention;

FIGURE 4 is a block diagram that illustrates the operations of a verification device according to the present invention;

FIGURE 5 is a block diagram that illustrates the operations of a key recovery device using master keys;

FIGURE 6 is a schematic representation of an embodiment of the present invention for securing card payments accepted over the Internet;

FIGURE 7 is a schematic representation of an embodiment of the present invention for securing card payments made at a point of sale using a mobile payment device;

FIGURE 8 is a flow chart that illustrates the procedure undertaken by a merchant accepting payment transactions secured by means of a TVC; and

FIGURE 9 is a flow chart that illustrates the procedure undertaken by a card issuer authorizing payment transactions secured by means of a TVC.

DESCRIPTION OF THE EMBODIMENTS

FIGURE 1 shows a system that is comprised of three main components referred to as a personal transaction device (PTD) **100**, a transaction system **110**, and a verification system **120**. The verification system **120** is further comprised of a verification device **121**, a key management device **122**, and an issuance device **123**.

Usually under the control of a user attending a point-of-service of the transaction system **110**, the PTD **100** is used for authentication of the transactions originated by the user. The PTD **100** has storage and processing capacities, and consists, for example, of a computer system, a smart card, a mobile phone, a personal digital assistant, or a combination thereof. A PTD **100** may either be intended for a single purpose or may consist of a generic platform capable to operate with a plurality of transaction systems **110** or verification systems **120**. For sake of understanding, the following descriptions assume a single purpose device.

According to the present invention, the PTD **100** is used for storage and concealment of a secret device key **201** known only to the PTD **100** and the verification system **120**. Along with the device key **201**, the PTD **100** stores identification information **221** and other attributes **222**, and is capable of performing the algorithms necessary to the production of a TVC according to the method depicted **FIGURE 3**. The series of attributes **222** includes, for example, an expiration date, a user's name, or any other information necessary to conduct transactions with the transaction system **110.**

According to the present invention, the PTD **100** must be initialized before use. This procedure, formally referred to as the issuance step, consists of an exchange of information between the PTD **100** and the verification system **120** under the control of the issuance device **123**. The issuance step consists either of a download **501** of the identification information **221**, the device key **201**, and the initial series of attributes **222** from the verification system **120** to the PTD **100**, registration **502** of these pieces of information from the PTD **100** into the verification system **120**, or a combination thereof. The details of the procedure utilized during the issuance step are not material to the present invention, and one skilled in the art can identify numerous implementations including, for example, the systems and procedures used in the manufacture of smart cards, the issuance and electronic delivery of virtual cards, or the registration of keying material with a central authority.

The key management device **122** is the component used by the verification system **120** to manage the device keys **201** in use by the PTDs **100** associated with the verification system **120**. The key management device **122** has storage and computational capacities, and consists of, for example, a computer system, a hardware security module, or a combination thereof. The key management device **122** operates in concert with the issuance device **123** and the verification device **121**. It is responsible for the storage and concealment of the secret bits of information **203** necessary to recover or generate the device keys **201**, and is capable of performing the algorithms necessary to these operations. In one embodiment, the device key **201** associated with each PTD **100** is simply stored on a secure storage medium accessible by the key management device **122**. Recovery of a device key **201** consists of retrieving the key from the storage medium using, for example, the identification information **221** associated with the PTD **100**. In another embodiment, the device keys **201** are encrypted by means of the secret bits of information **203** known only to the key management device **122** and stored on a non-secure storage medium. Recovery of a device key **201** consists of retrieving the encrypted device key from the storage medium, and decrypting the encrypted device key using the secret bits of information **203**. In another embodiment, the device keys are derived from the secret bits of information **203** known only to the key management device **122**. This preferred embodiment is further described in **FIGURE 5**.

The verification device **121** is the component used by the verification system **120** to ascertain the origin and the integrity of a transaction. The verification device **121** is capable of performing the verification method illustrated in **FIGURE 4**, and consists of, for example, a computer system, a hardware security module, or a combination thereof.

In a transaction, the transaction system **110** submits an authentication request **511** to the PTD **100** regarding a service request initiated by a user. Upon approval of the authentication request **511** by the user, the PTD **100** computes a TVC from characteristic parameters of the transaction and a secret device key **201** that is shared with a verification system **120**. Such characteristic parameters include certain parameters contained in the authentication request **511** and, for example, the identification information **221** and certain attributes **222** stored in the PTD **100**. The PTD **100** then inserts the TVC, the identification information **221**, and other pieces of information necessary to verify the TVC into an authentication response **512** that is returned to the transaction system **110**. In order to ascertain the validity of the authentication response **512**, the transaction system **110** refers to the verification system **120** submitting a verification request **513** constructed from the

authentication response **512** returned by the PTD **100** and other pieces of information **231** that may be necessary to the verification system **120**. By leveraging the identification information **221** inserted into the verification request **513** and other information **211** or secret bits of information **203** available locally, the verification system **120** recovers the key used in the computation of the TVC by the PTD **100**. The verification system **120** then reconstructs the set of characteristic parameters authenticated by the PTD **100** and computes a second TVC that is compared with the TVC inserted into the verification request **513**. Upon completion, the verification system **120** returns a verification response **514** to the transaction system **110** indicating whether the TVC is valid with regard to the transaction and its intended origin.

When the present invention is intended to progressively replace traditional static verification codes, the transaction system **110** must be adapted to either distinguish the transactions secured by means of a TVC, or implement a redundant verification procedure.

There are several solutions to make explicit the use of a TVC while trying to minimize changes to legacy transaction systems **110**. One of them consists of defining a transaction marker by specifying a new constant value for an existing bit of information. For example, the authorization protocol used by one of the major credit card company specifies a one-byte marker to indicate the means used for capture of the card verification code. By specifying a new constant value for this marker, the authorization protocol could convey sufficient bits of information to distinguish TVC from traditional card verification codes.

Less explicit alternatives may also be considered. Sometimes, contextual bits of information may be sufficient for distinguishing between TVCs and traditional verification codes. For example, a card issuer may limit the use of TVCs to transactions made with a surrogate card number. Thereupon, distinguishing between surrogate card numbers and traditional card numbers is sufficient to recognize the transactions secured by means of a TVC.

In those instances where the transaction system **110** cannot be adapted to distinguish TVC from traditional static verification codes, the transaction system **110** must adopt a redundant verification procedure. In this process, the verification procedure consists of a first verification assuming that the verification code is either a TVC or a static verification code. If that attempt fails, then the verification is tried one more time assuming that the verification code is of the other type. If either attempt succeeds, the transaction is authenticated. If both fail, the transaction is deemed invalid.

FIGURE 2 is a block diagram that illustrates the method used for computation of a TVC **400** according to the present invention. Upon entry, the method receives the set of transaction parameters **500** to be authenticated and the transaction key **200** to be used for authentication. The method consists of computing a cryptographic authentication code **401** in an authentication step **301**, compressing the authentication code **401** in a compression step **302**, and encoding the compressed authentication code **402** in an encoding step **303**.

In the authentication step **301**, a cryptographic algorithm is applied to the transaction parameters **500** using the transaction key **200**. The output of the authentication step **301** consists of a series of bits whose configuration is representative of the transaction key **200** and the transaction parameters **500**, though it does not reveal any information regarding the value of the transaction key **200**. The details of the algorithm used in the authentication step **301** are not material to the present invention and numerous implementations have been documented in the prior art. One knowledgeable in the field of cryptography can identify several algorithms that could serve the present purpose, including, for example, CBC-MAC and RIPE-MAC.

The compression step **302** consists of reducing the length of the authentication code **401** generated in the authentication step **301**. The compression step **302** may be necessary to comply with the length requirements set forth by the transaction system **110**. The algorithm used for compression does not impair the cryptographic properties of the authentication code **401**, but merely reduces its value space, which reduction shall be compensated by, for example, monitoring verification failures and blacklisting a PTD **100** suspected to be under attack. If the cryptographic algorithm used in the authentication step **301** is adequate, the compression step **302** may be limited to a simple truncation of the authentication code **401**. The compression step **302** results in the compressed authentication code **402**.

The encoding step **303** consists of translating the compressed authentication code **402** into a series of characters that comply with the syntactical requirements set forth by the transaction system **110**. A translation may be performed, for example, by replacing each byte in the compressed authentication code **402** by modulo indexing into a translation table containing the characters allowed by the transaction system **110**. When using this method, each byte of the compressed authentication code **402** is assumed to be an unsigned integer value (0-255) and used to index modulo the size of the table of characters that comply with the syntactical requirements of the transaction system **110**. The character value located at the

given index in the table of characters is used in place of the original byte, and the concatenation of the respective characters is the TVC **400**.

According to the present invention, the compression step **302** and encoding step **303** must be considered in concert rather than independently. For example, the compression algorithm used in the compression step **302** may have to account for further compression or expansion resulting from the encoding algorithm used in the encoding step **303**.

In a particular embodiment of the present invention intended for authentication of a card transaction, computation of the TVC **400** results in a 3 or 4 digit alphanumeric value having an alphabetic character in a fixed position, for example, the first position. This alphabetic character can be used to distinguish a TVC from traditional card verification codes. Such a result could be obtained by truncation of the authentication code **401** and encoding of the truncated authentication code **402** by means of the procedure described in the encoding step **303** using a translation table that contains the characters (A-Z) followed by the characters (0-9). The first byte of the truncated authentication code **402** is encoded by indexing modulo 26, resulting in an alphabetic character, while the remaining characters are encoded by indexing modulo 36.

FIGURE 3 is a block diagram that illustrates the operations of a PTD **100** according to the present invention. In a transaction, the PTD **100** is provided with an authentication request **511**, which conveys information relevant to the transaction initiated by the user. The PTD **100** then proceeds with a device activation step **310**, a transaction key generation step **320**, a parameters encoding step **330**, and a TVC computation step **340**.

In the preferred embodiment, the PTD **100** is protected from unauthorized uses whether they arise out of an unauthorized user or a bogus transaction system **110**. To that end, in the device activation step **310**, the identity of the user is verified and the user prompted to confirm his intend regarding the transaction being authenticated. The identity of the user can be verified by, for example, the use of a lock, which would forbid the use of the PTD **100** unless the user is successfully authenticated. The details of the features used for authentication of the user are not material to the present invention and one skilled in the art could identify several implementations including, for example, the use of a secret PIN or the verification of biometric characteristics.

The transaction key generation step **320** consists of deriving the transaction key **200** to be used for computation of the TVC **400** for the current transaction. The transaction key **200** is derived from the device key **201** by means of an algorithm and a block of information

811 constructed from, for example, certain parameters of the authentication request **511**, the identification information **221** associated with the PTD **100**, and certain attributes **222** stored in the PTD **100**. These attributes **222** may include an internal register **223** that consists of, for example, a pseudo-random number generated for the purpose of the current transaction or a sequence number that is incremented for each transaction, such as those used in a check processing system. It has been established in the prior art that the generation of a transaction key **200** in the manner described in the transaction key generation step **320** enhances the immunity of the device key **201** to attacks. The details of the algorithm used in the transaction key generation step **320** are not material to the present invention and numerous implementations have been documented in the prior art. In those instances where the PTD **100** or the transaction system **110** cannot accommodate the use of a transaction key **200** derived from the procedure described in the transaction key generation step **320**, the device key **201** is used as the transaction key **200**.

The parameters encoding step **330** consists of the collection and normalization of the transaction parameters **500** to be authenticated, which are comprised of certain parameters of the authentication request **511**, and other pieces of information deemed necessary to securing the transaction such as, for example, the identification information **221** associated with the PTD **100** and certain attributes **222** stored in the PTD **100**. The collection of these transaction parameters **500** may require further interactions with the user. To assist in the prevention of replay-attacks, the authenticated transaction parameters **500** preferably contain some unique bit of information such as, for example, a unique transaction identifier or a transaction timestamp.

Finally, the TVC computation step **340** utilizes the transaction parameters **500** resulting from the parameters encoding step **330** and the transaction key **200** resulting from the key generation step **320** to compute the TVC **400** according to the method illustrated **FIGURE 2.**

Upon completion, the PTD **100** outputs an authentication response **512**, which includes the TVC **400** and the identification information **221** associated with the PTD **100**, as well as any other pieces of information necessary to the verification of the TVC including, for example, the contents of the register **223** used during generation of the transaction key **200**.

Alternative embodiments of the present invention may adopt additional steps such as, for example, recording the transactions to some storage medium.

FIGURE 4 is a block diagram that illustrates the operations of a verification device **121** according to the present invention. In a transaction, the verification device **121** is provided with a verification request **513**, which includes, among other parameters, the TVC **410** to be verified and the identification information **221** associated with the PTD **100** used for authentication of the transaction. The verification device **121** then proceeds with a device key recovery step **350**, a transaction key recovery step **360**, a parameters encoding step **370**, a TVC computation step **380**, and a TVC validation step **390**.

In the device key recovery step **350**, the device key **201** associated with the PTD **100** that initiated the transaction is recovered by submitting a recovery request **812** to the key management device **122**. The recovery request **812** is constructed from certain parameters of the verification request **513**, including the identification information **221** associated with the PTD **100**, and other pieces of information **211** available to the verification system **120**. In the preferred embodiment, the means used for communication with the key management device **122** is protected from prying eyes as to prevent disclosure of the device key **201**.

The transaction key recovery step **360** consists of recovering the transaction key **200** used by the PTD **100** that originated the TVC **410**. The transaction key **200** is derived by means of an algorithm from the device key **201** recovered in the device key recovery step **350** and a block of information **811** that includes, for example, certain parameters of the verification request **513** and the other pieces of information **211** available to the verification system **120**. The algorithm employed in the transaction key recovery step **360** is consistent with the algorithm used in the transaction key generation step **320** in **FIGURE 3**.

The parameters encoding step **370** consists of the collection and normalization of the authenticated transaction parameters **500**, which are collected from the verification request **513** and the other pieces of information **211** available to the verification system **120**. The encoding process used in the parameters encoding step **370** is consistent with the process used in the parameters encoding step **330** in **FIGURE 3**.

In the TVC computation step **380**, the transaction key **200** resulting from the transaction recovery step **360** and the transaction parameters **500** resulting from the parameters encoding step **370** are used to generate the TVC **400** according to the procedure illustrated in **FIGURE 2**.

In the TVC validation step **390**, the TVC **400** computed by the verification device **121** is compared to the TVC **410** provided on entry in the verification request **513**. Upon

completion, the verification device **121** returns a verification response **514** that consists primarily of a return code indicating whether the two codes match.

An alternative embodiment of the present invention may include additional steps such as, for example, recording the transactions to some storage medium.

FIGURE 5 is a block diagram that illustrates the operations of a key recovery device using master keys. The operations described herein are employed when the device key **201** is derived from the secret bits of information **203** known only to the key management device **122**. The secret bits of information **203** consist of a series of master keys, from which the device keys **201** associated with the PTDs **100** are derived. Although it would be possible to make use of a single master key, it is preferable for security and maintenance reasons to maintain a plurality of master keys. New master keys can be generated as older keys expired.

In the preferred embodiment, the key recovery process is comprised of two steps referred to as the master key selection step **351** and the key recovery step **352**.

In the master key selection step **351**, the master key **204** that has been used for generation of the device key **201** is selected from the series of master keys **203**. The master key **204** may be selected by, for example, indexing the set of master keys **203** using some properties of the PTD **100** such as, for example, an expiration date, an identifier, a class, or any combination thereof. The properties used for indexing are derived from certain parameters of the recovery request **812** and other pieces of information **211** available to the verification system **120**.

In the device key recovery step **352**, a cryptographic algorithm is used to derive the device key **201** associated with the PTD **100** from the master key **204** and other characteristic properties of the PTD **100** derived from certain parameters of the recovery request **812** and other pieces of information **211** available to the verification system **120**. The cryptographic algorithm may be, for example, a one-way hash function such as SHA-1. The series of bits that results from said computation may be further adjusted to conform to the key requirements set forth by the algorithm used in the authentication step **301**. The details of the algorithm contemplated herein are not material to the present invention, and numerous implementations have been documented in the prior art.

FIGURE 6 is a schematic representation of an embodiment of the present invention for securing card payments accepted over the Internet. The buyer **10** selects goods for purchase online through the use a Web browser running on a terminal **111**. After selection of the goods, the buyer **10** is prompted by, for example, a button labeled "CHECKOUT,"

which, when clicked by the buyer **10**, invokes a procedure through which the buyer **10** is asked to provide personal, shipping, and payment information. The method by which the merchant **20** obtains the payment information from the buyer **10** is not material to the present invention and numerous implementations have been documented in the prior art.

In the preferred embodiment, the buyer **10** invokes the payment procedure by clicking on a button that directs the Web browser on the terminal **111** to a payment server **112** operated by or on behalf the merchant **20**. In response, the payment server **112** returns an HTML page **611** that contains input fields to collect the payment information from the buyer **10** and output fields to specify the payment parameters. The input fields provide for collection of the account number, the account name, the expiration date, and the verification code of the card being used for the payment, while the output fields specify, for example, the payment brands accepted by the merchant **20**, the merchant's **20** account information for each of said brands, a timestamp for the transaction, a total sale amount, and a currency type.

A virtual wallet application is launched, which recognizes and extracts the payment parameters from the HTML page **611**, which are presented to the buyer **10** for review. Upon approval of the payment parameters by the buyer **10**, the virtual wallet application prompts the buyer **10** for a payment device **101**, assumed as the PTD **100** in this particular embodiment. Once the payment device **101** is activated, the virtual wallet application inserts the amount of the purchase and the account information of the merchant **20** with other relevant payment information into an authentication request **511** that is submitted to the payment device **101**. The payment device **101** computes the TVC according to the procedure illustrated **FIGURE 3**. Upon completion, the payment device **101** returns the TVC along with other relevant card information in the authentication response **512**. The virtual wallet application transfers these pieces of information into their respective input field on the HTML page **611**, resulting in the payment response **612** that is returned to the payment server **112**.

FIGURE 8 illustrates the procedure utilized by the merchant **20** to process payment transactions according to the present invention. The merchant **20** first determines if the payment transaction is secured by means of a TVC by verifying whether the first character of the verification code (if present) is alphabetical or numerical. When alphabetical, the merchant **20** is assured that authorization by the issuer **40** would be sufficient to ascertain the legitimacy of the payment. In such circumstances, the merchant **20** can safely forgo current fraud screening procedures.

The request for authorization **613** for a transaction authenticated by means of a TVC is similar in every respect to a request for authorization having a traditional card verification code. In other words, the merchant **20** submits the TVC for verification by placing said TVC into the field intended for traditional static verification codes.

Returning to **FIGURE 6**, traditional card authorization requests are intermediated by a third-party known as an acquirer **30**. In general, the present invention is transparent to the acquirer **30** unless, for example, the acquirer **30** has adopted syntactical restrictions for the verification codes. Otherwise, unaware that the transaction is making use of a TVC, the acquirer **30** forwards the payment information **614** for authorization to the issuer **40** in the same manner as would occur in a traditional transaction.

FIGURE 9 illustrates the procedure utilized by the issuer **40** to authorize a payment transaction according to the present invention. Upon receipt of the payment information **614** from the acquirer **30**, the issuer **40** identifies those transactions secured by means of a TVC and undertakes the verification steps illustrated **FIGURE 4** as well as steps necessary to compensate the reduction of the value-space that results from the compression step **302**. Preferably, the authorization procedure monitors verification failures, which may result from brute-force attacks against the TVC or the device key **201**, and automatically deactivates a card that appears to be the subject of an attack. Further authorization requests are systematically rejected until the issuer **40** reactivates the card.

Returning to **FIGURE 6**, once the issuer **40** completes the authorization procedure, having verified the TVC using the verification system **120**, the issuer **40** returns an authorization response **615** to the acquirer **30**, which, in turn, returns the authorization response **616** to the merchant **20**. Finally, the buyer **10** receives notification **617** of the authorization or denial of the payment transaction through the Web browser running on the terminal **111**.

FIGURE 7 is a schematic representation of an embodiment of the present invention for securing card payments made at a point of sale using a mobile payment device **102**. As the merchant **20** rings the total of the purchase on the cash register **113**, the buyer **10** declares his intend to pay with his mobile payment device **102**, assumed as the PTD **100** in this embodiment. The merchant **20** invokes a procedure by which a data communication link is established between the cash register **113** and the mobile payment device **102**. The cash register **113** inserts the amount of the purchase and the account information of the merchant

20 with other relevant payment information into an authentication request **511** that is submitted to the mobile payment device **102**.

The mobile payment device **102** notifies the buyer **10** that an authentication request **511** for a payment has been received, and requests an approval from the buyer **10**. Upon approval by the buyer **10**, the mobile payment device **102** generates a TVC according to the method illustrated **FIGURE 3**, which is inserted with other relevant card information into the authentication response **512** that is returned to the cash register **113**.

The merchant **20** then obtains an authorization from the issuer **40** that issued the payment device **102** to the buyer **10**. This procedure is similar in every respect to the authorization procedure described in **FIGURE 6**. Once the authorization response **616** is received from the acquirer **30**, the cash register **113** completes the payment transaction by forwarding a notification **617** of the authorization or denial of the payment transaction to the mobile payment device **102**. The mobile payment device **102** terminates the communication link with the cash register **113** and concludes the payment transaction.

Although the present invention has been described herein in conjunction with the appended drawings, those skilled in the art will appreciate that the scope of the present invention is not so limited. Many variations are possible without departing from the spirit and scope set forth in the claims. For example, an implementation of the present invention may concede additional changes such as increasing the length of traditional verification codes when making use of a TVC and/or defining new data elements in the protocols to convey or make explicit usage of a TVC.

The present invention has been described herein in term of functional blocks and various processing steps. It should be appreciated that such functional blocks may be realized by any number of hardware components configured to perform the specified function. For example, the verification system **120** may be realized into a single hardware component, or the functional blocks may be combined in many ways and realized into a plurality of hardware components. It should be further noted that the present invention might employ any number of conventional techniques for data transmission, training, signal processing and conditioning, and the like, which techniques are not necessarily detailed in the description of the present invention.

The disclosed system, method and devices have been disclosed by reference to its preferred embodiments. Those of ordinary skill in the art will understand that additional embodiments of the disclosed system, method and devices are made possible by the foregoing

disclosure and that the emphasis on card authorization systems herein is merely one exemplary application of the present invention. Such additional embodiments shall fall within the scope and meaning of the appended claims.

CLAIMS

What is claimed is:

1. A system for ascertaining the integrity and the origin of a transaction at a point of initiation of the transaction, said system comprising:

(a) means for creating a transaction dependent verification code at the point of initiation of the transaction, said means for creating a transaction dependent verification code including:

(i) a cryptographic authentication code computed from a shared secret parameter and a transaction dependent parameter;

(ii) means for compressing said cryptographic authentication code;

(iii) means for encoding said cryptographic authentication code;

(b) means for verifying said transaction dependent verification code;

whereby the integrity and the origin of said transaction is ascertained by the successful verification of said transaction dependent verification code by said means for verifying said transaction dependent verification code.

2. A method for ascertaining the integrity and the origin of a transaction at a point of initiation of the transaction, said method comprising the steps of:

(a) creating a transaction dependent verification code at the point of initiation of the transaction, said step of creating a transaction dependent verification code including:

(i) computing a cryptographic authentication code computed from a shared secret parameter and a transaction dependent parameter;

(ii) compressing said cryptographic authentication code;

(iii) encoding said cryptographic authentication code;

(b) verifying said transaction dependent verification code;

whereby the integrity and the origin of said transaction is ascertained to be authentic by the successful verification of said transaction dependent verification code by said means for verifying said transaction dependent verification code.

3. A device for authenticating a transaction, said device tangibly embodying a storage device and a program of executable instructions to perform method steps for authenticating a transaction, said device comprising:

means for generating an authentication code;

means for compressing said authentication code to comply with the length requirements for verification codes used in traditional transactional systems;

means for encoding said authentication code to comply with the syntax requirements for verification codes used in traditional transactional systems; and

whereby said compressed, encoded verification code is used in lieu of static verification codes commonly used in traditional transactional systems.

4. A device for authenticating a transaction, said device tangibly embodying a storage device and a program of executable instructions to perform method steps for authenticating a transaction, said device comprising:

means for recovering the cryptographic key used during the authentication process for said transaction;

means for using said cryptographic key and informational parameters to calculate the transaction-dependent verification code;

means for authenticating said transaction-dependent verification code by comparing said transaction-dependent verification code to a verification code provided as part of the transaction; and

generating a signal dependent upon the result of said authentication.

5. A system for ascertaining the integrity and origin of a transaction, said system comprising:

authentication means for creating a transaction dependent verification code at the point of service of the transaction;

said authentication means including:

means for computing a cryptographic authentication code from a shared secret parameter and at least a transaction dependent parameter;

means for compressing said cryptographic authentication code;

means for encoding said cryptographic authentication code;

verification means for verifying said transaction dependent verification code;

whereby the origin and integrity of said transaction is ascertained to be authentic by the successful verification by said verification means of said transaction dependent verification code created by said authentication means.

6. A method for ascertaining the integrity and origin of a transaction, said method comprising the steps of:

creating a transaction dependent verification code at the point of service of the transaction;

said step of creating a transaction dependent verification code including:

computing a cryptographic authentication code computed from a shared secret parameter and a transaction dependent parameter;

compressing said cryptographic authentication code;

encoding said cryptographic authentication code;

verifying said transaction dependent verification code;

whereby the origin and integrity of said transaction is ascertained to be authentic by the successful verification of said transaction dependent verification code.

7. A device for authenticating a transaction at a point of service of a transaction system, said device tangibly embodying a storage device and a program of executable instructions to perform method steps for authenticating a transaction, said device comprising:

means for generating an authentication code;

means for compressing said authentication code to comply with the length requirements of said transaction system;

means for encoding said authentication code to comply with the syntax requirements of said transaction system; and

whereby said compressed and encoded authentication code is used as a transaction dependent verification code to ascertain the origin and the integrity of the transaction.

8. A device for verifying the origin and integrity of a transaction using a transaction dependent verification code, said device tangibly embodying a storage device and a program of executable instructions to perform method steps for verifying the authenticity of a transaction, said device comprising:

means for recovering the cryptographic key used during the authentication process for said transaction;

means for using said cryptographic key and informational parameters to calculate the transaction-dependent verification code;

means for authenticating said transaction-dependent verification code by comparing said transaction-dependent verification code to a verification code provided as part of the transaction; and

generating a response message dependent upon the result of said verification.

9. A system for ascertaining the origin and the integrity of a transaction, said system comprising:

authentication means for creating a transaction dependent verification code at a point of service of said system, said means including:

memory means for storage of at least a secret parameter and an identification parameter;

means for receiving transaction parameters;

a program of executable instructions;

means for processing said program of executable instructions, said secret parameter, and said transaction parameters to produce a transaction verification code;

means for outputting at least said transaction verification code and said identification parameter.

verification means for verifying a transaction dependent verification code, said means including:

means for receiving transaction parameters, said transaction parameters including at least an identification parameter and a first transaction verification code;

a first program of executable instructions;

means for processing said first program of executable instructions and said identification parameter to recover the secret parameter stored into the authentication means associated with said identification parameter;

a second program of executable instructions;

means for processing said second program of executable instructions, said recovered secret parameter, and said transaction parameters to produce a second transaction verification code;

means for comparing said first transaction verification code and said second transaction verification code;

means for outputting the result of said comparison.

whereby production of a transaction verification code using a secret parameter and transaction parameters consists of:

an authentication step for computing a cryptographic authentication code from said secret parameter and said transactions parameters;

a compression step for compressing said cryptographic authentication code;

an encoding step for encoding said cryptographic authentication code;

Whereby the origin and integrity of said transaction is verified if the output of said verification means indicates that comparison of said first transaction verification code and said second transaction verification code was successful.

10. The system as is claim 9, wherein a copy of the secret parameter stored in said authentication means is stored in said verification means.

11. The system as is claim 9, wherein the secret parameter stored in said authentication means is derived from a second secret stored in said verification means using pieces of information related to said authentication means.

12. The system as is claim 9, wherein said compression step is optional.

13. The system as is claim 9, wherein said encoding step is optional.

14. The system as in claim 9, wherein said verification means monitors verification failures and systematically denies verification of the transactions originated from said authentication means when said verification failures for said authentication means exceeds a given threshold parameter.

15. The system as in claim 9, wherein said authentication means is a computer system, a smart card, a mobile telephone, a personal digital assistant, or a combination thereof.

16. The system as in claim 9, wherein said verification means is a computer system, a hardware security module, or a combination thereof.

17. The system as in claim 9 used in connection with the authorization of account-based payment transactions, wherein:

said transaction parameters consists at least of a currency amount and the account number of the payee or a surrogate of said account number;

said identification parameter is the account number of the payer or a surrogate of said account number;

18. The system as in claim 17 used in connection with the authorization of card payment transactions wherein:

said payment transactions are traditionally secured by means of a card verification code;

said transaction verification code is compliant with traditional card verification code standards and used in place of said traditional card verification code.

19. The system as in claim 17 used in connection with the authorization of card payment transactions wherein:

said payment transactions are traditionally secured by means of a personal identification number;

said transaction verification code is compliant with traditional personal identification number standards and used in place of said traditional personal identification number standards.

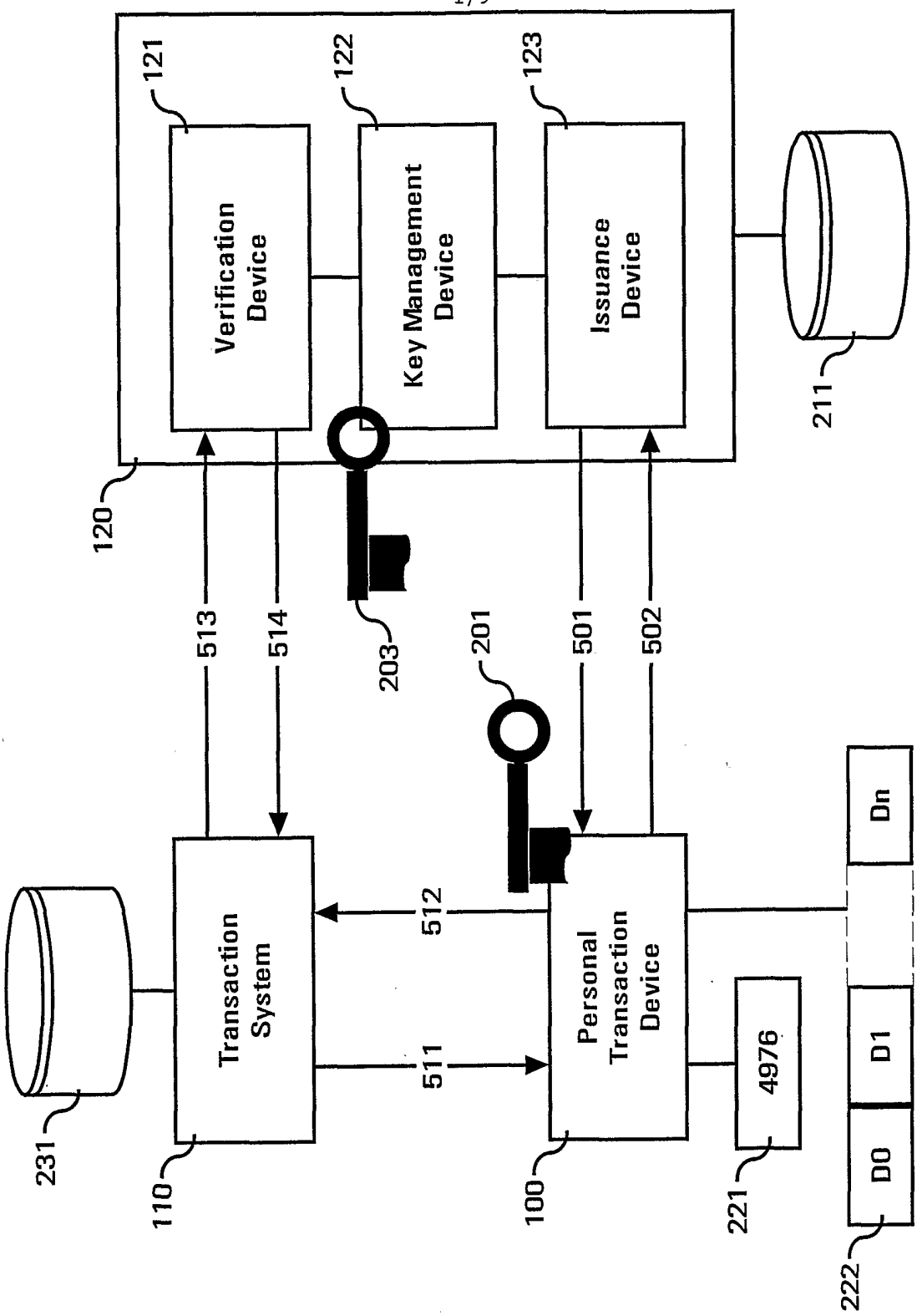

121
122
123
Verification Device
Key Management Device
Issuance Device
211
120
513
514
203
201
501
502
Transaction System
512
511
Personal Transaction Device
Dn
D1
D0
4976
231
110
100
221
222

FIGURE 1

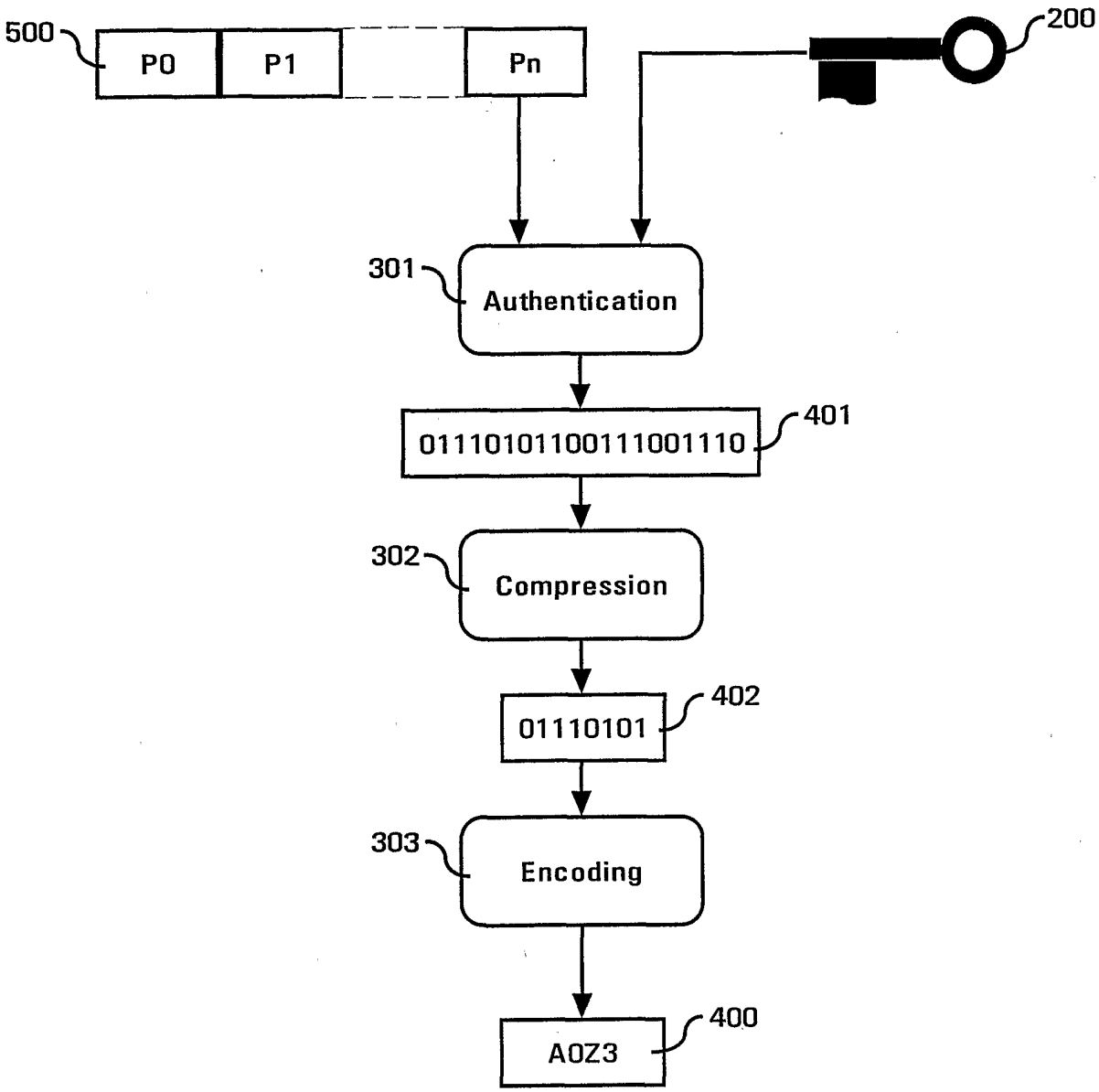

500
P0
P1
Pn
200
301
Authentication
01110101100111001110
401
302
Compression
01110101
402
303
Encoding
A0Z3
400

FIGURE 2

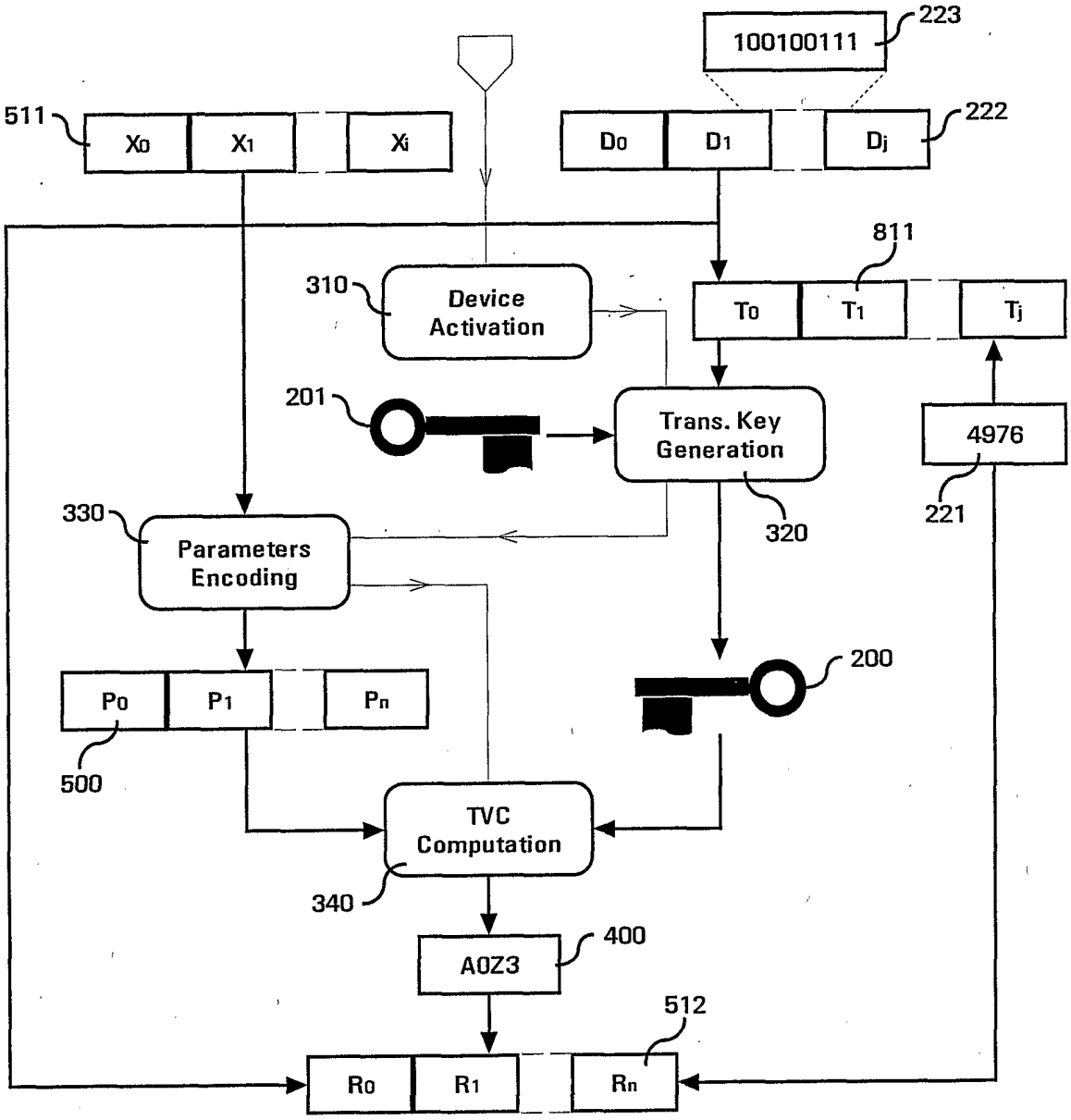

100100111
223
511
X0
X1
Xi
D0
D1
Dj
222
811
310
Device Activation
T0
T1
Tj
201
Trans. Key Generation
4976
330
Parameters Encoding
320
221
200
P0
P1
Pn
500
TVC Computation
340
400
A0Z3
512
R0
R1
Rn

FIGURE 3

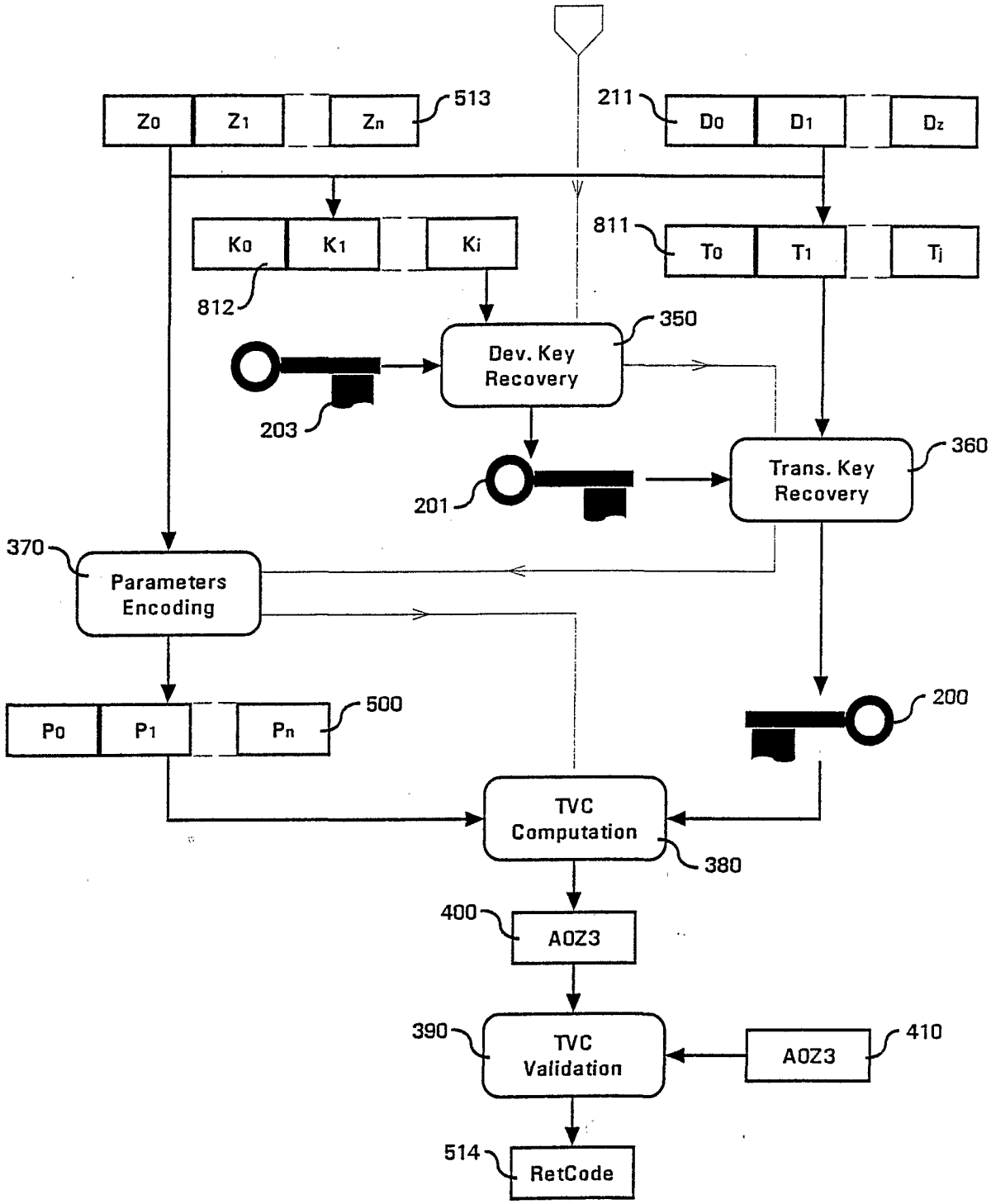

Z0
Z1
Zn
513
211
D0
D1
Dz
K0
K1
Ki
812
811
T0
T1
Tj
350
Dev. Key Recovery
203
201
360
Trans. Key Recovery
370
Parameters Encoding
P0
P1
Pn
500
200
TVC Computation
380
400
AOZ3
390
TVC Validation
AOZ3
410
514
RetCode

FIGURE 4

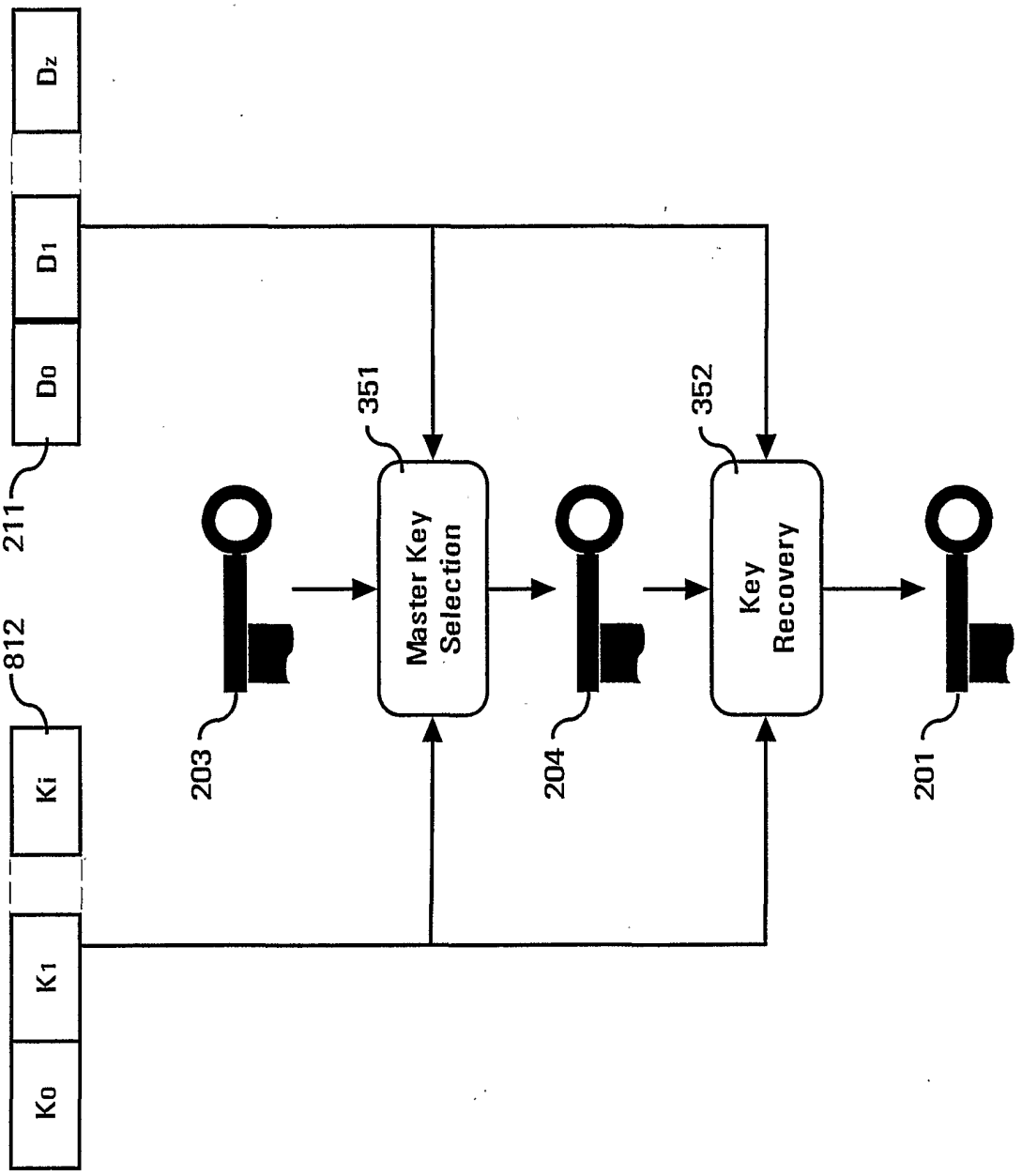

Dz
D1
Do
211
812
Ki
K1
Ko
203
351
Master Key Selection
204
352
Key Recovery
201

FIGURE 5

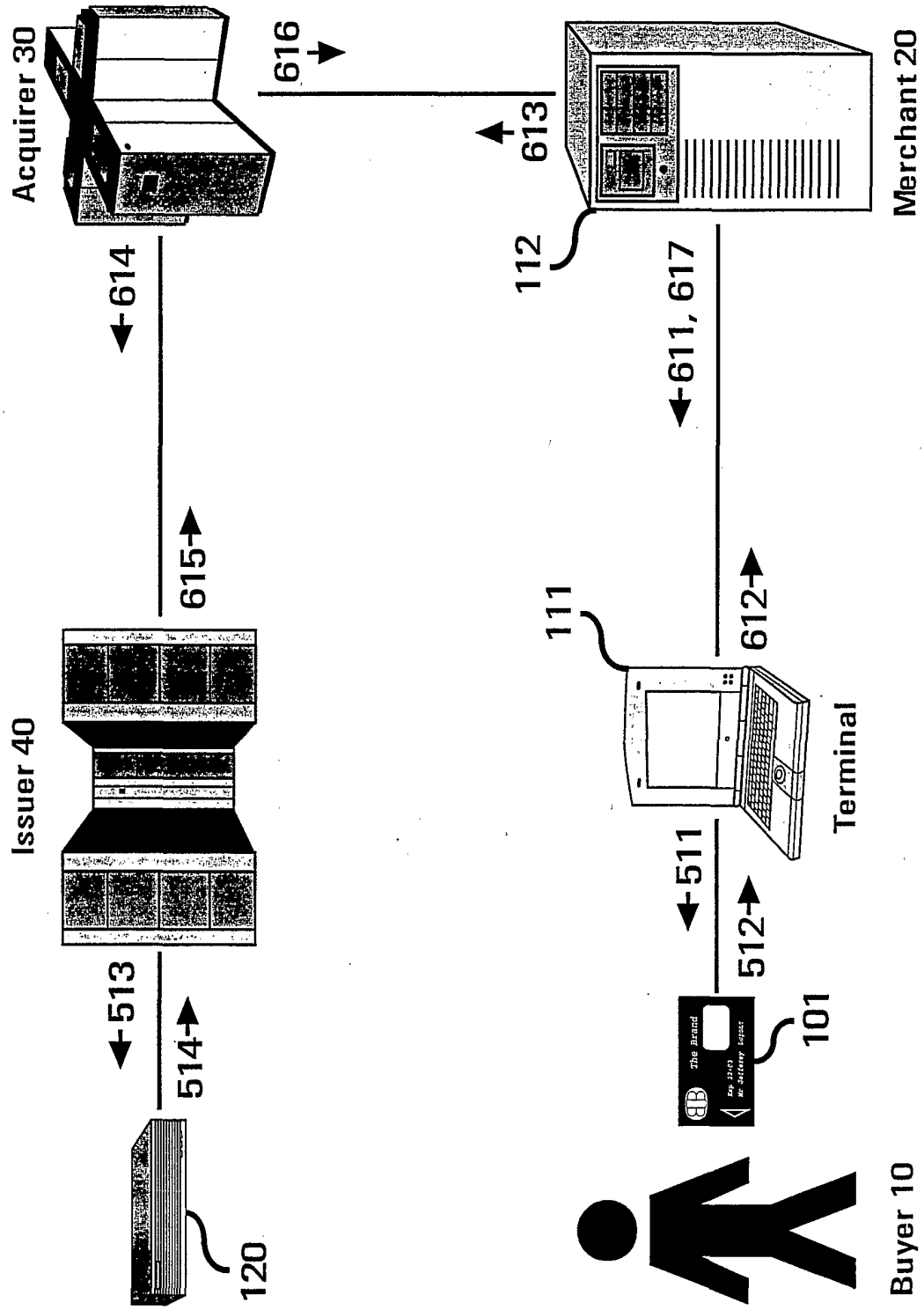

Acquirer 30
616
613
Merchant 20
112
614
611, 617
615
111
612
Issuer 40
Terminal
511
513
514
512
101
120
Buyer 10

FIGURE 6

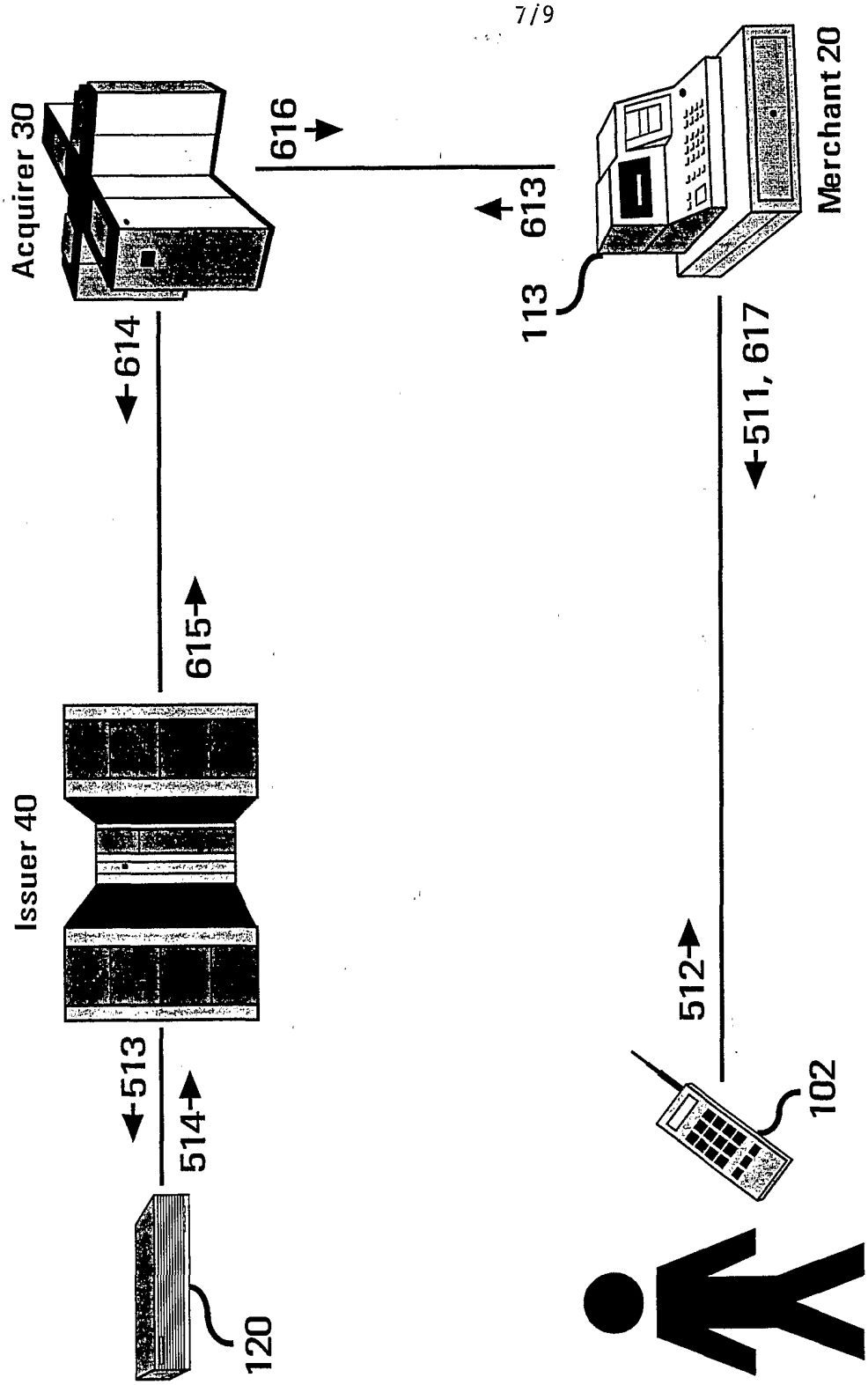

Acquirer 30
616
613
Merchant 20
113
614
511, 617
615
Issuer 40
513
514
512
120
102
Buyer 10

FIGURE 7

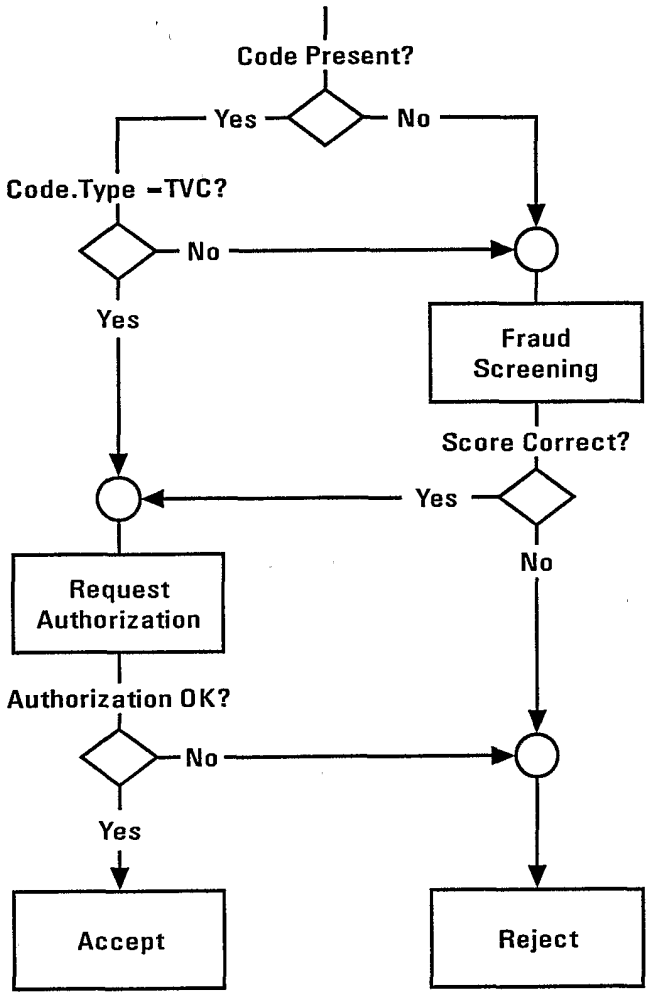

Code Present?
Yes
No
Code.Type =TVC?
No
Yes
Fraud Screening
Score Correct?
Yes
No
Request Authorization
Authorization OK?
No
Yes
Accept
Reject

FIGURE 8

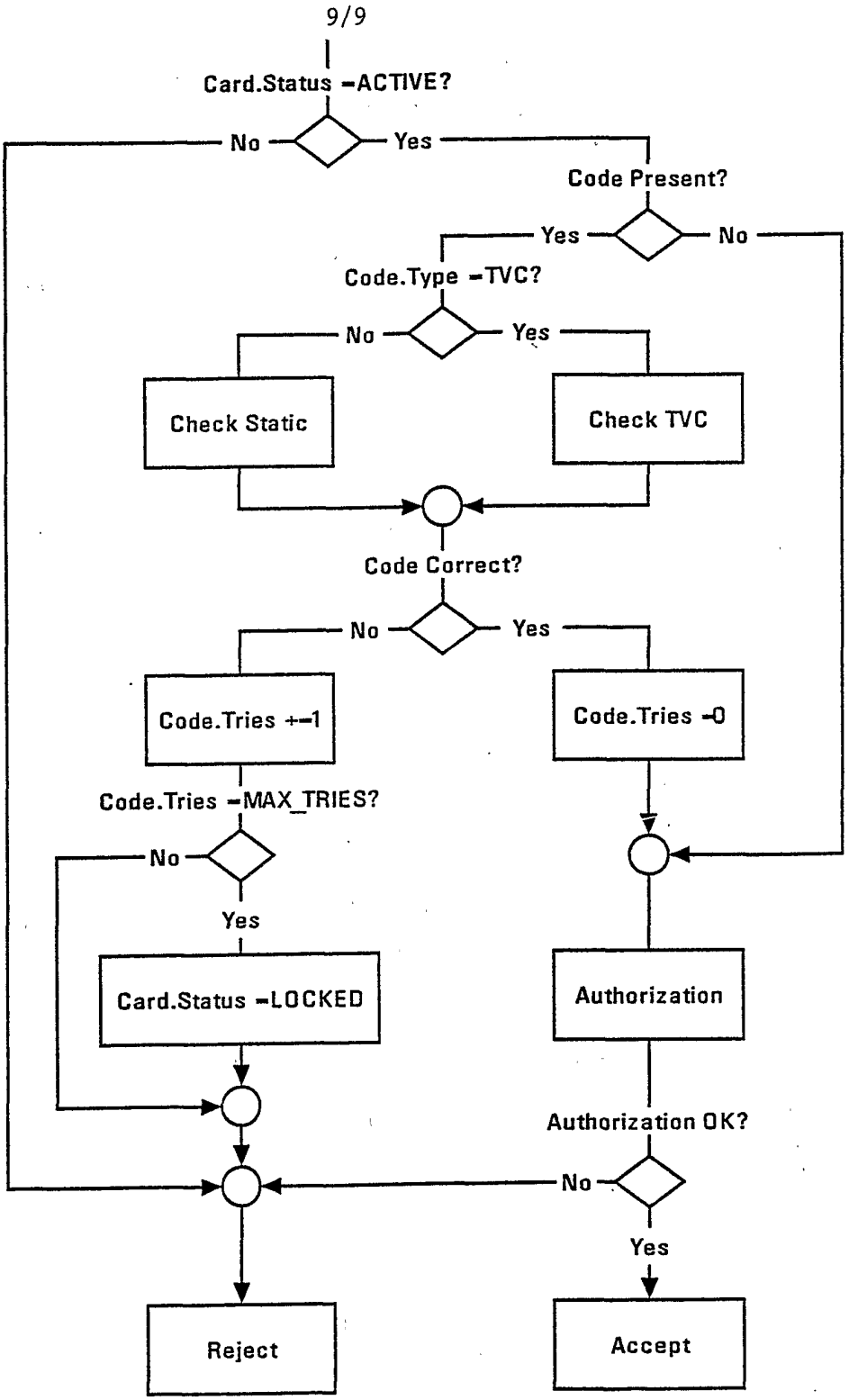

Card.Status =ACTIVE?
No
Yes
Code Present?
Yes
No
Code.Type =TVC?
No
Yes
Check Static
Check TVC
Code Correct?
No
Yes
Code.Tries +=1
Code.Tries =0
Code.Tries =MAX_TRIES?
No
Yes
Card.Status =LOCKED
Authorization
Authorization OK?
No
Yes
Reject
Accept

FIGURE 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/43635

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04L 9/00
US CL : 713/200

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/176-178,200;705/17, 26, 65,77,78

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 4,630,201 A (White)16 December 1986(19.061986), column6, lines 51-68, column 7 thru 8, lines 1-68, see alsocolumn 11, lines 40-67.	1-10,12-17 --- 11,18,19
Y	US 5,915,023 A (Bernstein) 22 June 1999 (22.06.1999), column 6, lines 8-13, col.7, lines 14-29, see also col. 13, lines 31-36	11
Y	US 5,317,636 A (Vizcaino) 31 May 1994 (31.05.1994), column 2, lines 37-65, column 5, lines 14-63.	18,19
Y,E	US 20020007320 A (Hogan et al) 17 January 2002 (17.01.2002), column 7, lines 6-24, Fig. 4a and 4b.	11, 18 and 19
Y, p	US 6,282,523 B1 (Tdesco et al) 28 August 2001 (28.08.2001), column 7, lines 43-65, column 14, lines 52-65.	1-10,12-17

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
07 February 2002 (07.02.2002)	15 MAR 2002
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O. Hayes Telephone No. (703) 305-4274

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.

PCT/US01/43635

Continuation of B. FIELDS SEARCHED Item 3:
WEST, DIALOG; search terms used; "transaction adj identifier or parameter or number", "electronic adj commerce", "electronic funds transfer" ," point of sale", "security or authentication code"